

Wednesday, May 7, 2025

Dear Staff,

We are writing to inform you of a recent development related to the cybersecurity incident PowerSchool experienced in December 2024.

PowerSchool is aware that a threat actor has reached out to multiple school district customers in an attempt to extort them using data from the previously reported December 2024 incident. PowerSchool does not believe this is a new incident.

Please be assured that both PowerSchool and Near North District School Board (NNDSB) are taking this situation very seriously. PowerSchool has informed us they are working with cybersecurity experts to thoroughly assess this development and have reported it to law enforcement in both Canada and the United States.

To date, NNDSB has not been contacted by the persons responsible for this attack.

As a reminder, as we shared with you on February 7, 2025, PowerSchool also offered and made widely available credit monitoring and identity protection services for a period of two years to NNDSB students and faculty regardless of whether they were individually involved. We encourage all those who were offered these services to take advantage of them:

· For individuals in Canada: <https://www.powerschool.com/security/sis-incident/notice-of-canada-data-breach/>

As was reported earlier this year, PowerSchool made the decision to pay a ransom because they believed it to be in the best interest of their customers and the students and communities they serve. As is always the case with these situations, there was a risk that the bad actors would not delete the data they stole, despite assurances and evidence that were provided to PowerSchool.

We wanted to share this update as part of our ongoing commitment to transparency. We remain committed to working closely with PowerSchool and law enforcement to provide support in any way we can.

Sincerely,
Near North District School Board